NPL 10799860

8/5/1 (Item 1 from file: 8)
DIALOG(R)File 8: Ei Compendex(R)

1210014948 **E.I. COMPENDEX No:** 20091512018879
Square hash with a small key size

Issue Title: Information Security and Privacy - 8th Australasian Conference, ACISP 2003, Proceedings
Heng, Swee-Huay; Kurosawa, Kaoru
Corresp. Author/Affil: Heng, S.-H.: Tokyo Institute of Technology, 2-12-1 O-okayama, Meguro-ku, Tokyo 152-8552, Japan
Corresp. Author email: shheng@crypt.ss.titech.ac.jp
Author email: kurosawa@cis.ibaraki.ac.jp
Conference Title: 8th Australasian Conference on Information Security and Privacy, ACISP 2003
Conference Location: Wollongong, NSW Australia **Conference Date:** 20030709-20030711
Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Lect. Notes Comput. Sci.) **(** Germany) 2003 2727 LNCS/- (522-531)
Publication Date: 20031201
Publisher: Springer Verlag
ISSN: 0302-9743 **eISSN:** 1611-3349
Item Identifier (DOI): 10.1007/3-540-45067-X-45
Document Type: Conference Paper; Book Series **Record Type:** Abstract
Language: English **Summary Language:** English
Number of References: 15
This paper shows an improvement of square hash function family proposed by Etzel et al. [5]. In the new variants, the size of keys is much shorter while the collision probability is slightly larger. Most of the main techniques used to optimize the original square hash functions work on our variants as well. The proposed algorithms are applicable to fast and secure message authentication. (c) 2003 Springer-Verlag Berlin Heidelberg.
Descriptors: Authentication; Security of data; *Hash functions
Identifiers: Collision probabilities; Key **sizes**; **Message** authentication codes; Secure **messages**; Square **hash**; Techniques used; Universal **hash**
Classification Codes:
723.2 (Data Processing)
723 (Computer Software, Data Handling & Applications)
921 (Applied Mathematics)

8/5/2 (Item 1 from file: 2)
DIALOG(R)File 2: INSPEC

09194084

Title: **Random walk based heuristic algorithms for distributed memory model checking**

Author(s): Hemanthkumar Sivaraj[1]; Ganesh Gopalakrishnan
Affiliation(s):
[1] Sch. of Comput., Utah Univ., Salt Lake City, UT, USA

Journal: Electronic Notes in Theoretical Computer Science , vol.89 , no.1
Publisher: Elsevier
Country of Publication: Netherlands
Publication Date: 2003
ISSN: 1571-0661
ISSN Type: print
U.S. Copyright Clearance Center Code: 1571-0661/2003/$30.00
URL: HTTP://WWW.ELSEVIER.NL/LOCATE/ENTCS/VOLUME89.HTML
Document Collection URL: HTTP://WWW1.ELSEVIER.COM/GEJ-NG/31/29/23/SHOW/PRODUCTS/NOTES/CONTENTS
Language: English
Document Type: Journal Paper (JP)
Treatment: Practical (P)

Abstract: We explore the use of distributed processing to enhance the performance of explicit state enumeration based safety model-checking. State enumeration based model-checkers employ a hash-table to cut off search when a state is revisited. Distributed model-checkers distribute this table across the processing nodes, employing inter-node messages to perform state lookups. This approach incurs the following penalties: hashing states, looking up hash-tables, and possibly exchanging messages. We study how to avoid these penalties in the context of safety model-checking, assuming that completeness can be sacrificed (acceptable for quick error detection). We employ the basic strategy of distributed random walk - a process of multiple processors randomly, and in an uncoordinated fashion, moving through the state-space looking for safety violations, without recording visited states. This process has the potential of maximizing CPU utilization, and consequently greatly increase the rate of state generation, as the pressure on the memory system as well as communication network is minimal. Moreover, the probability that a random-walk repeats the same sequence of moves can decrease exponentially with the length of the sequence; thus, the work wasted by occasionally repeating short sequences of searches may be more than offset by the increased state generation rate. Our choices are ideal for distributed systems that have low amounts of memory per node, and are interconnected by low bandwidth networks. We also explore techniques that backoff slightly from our extremal choices, by exploring heuristic combinations of breadth-first search (BFS) and random-walk (RW) that require a modest **amount** of **hash**-table lookup and **message** exchanges. These search methods are natural to combine, since BFS requires higher amounts of memory to maintain queues, but guarantees to find the shortest path to a state, while RW has the opposite characteristics. We first study these heuristic methods on synthetic benchmarks to gain sharper (more quantifiable) insights. We then conduct

studies on some realistic examples as well. We employ up to 10 single-processor CPUs that happen to be connected via 100BASE-T Ethernets. Our code was easily ported to other platforms, thanks to our use of the popular MPI distributed programming library. (*33 refs.*)

Subfile(s): C (Computing & Control Engineering)

Descriptors: data structures; distributed memory systems; distributed programming; formal verification; heuristic programming; message passing; table lookup; tree searching

Identifiers: random walk based heuristic algorithm; distributed memory model checking; state enumeration based model-checker; CPU utilization; communication network; breadth-first search; hash-table lookup; message exchanges; synthetic benchmarks; 100BASE-T Ethernets; MPI distributed programming library

Classification Codes: C6110F (Formal methods); C6120 (File organisation); C6150N (Distributed systems software); C4240C (Computational complexity)

International Patent Classification:
G06F-0009/44 (Arrangements for executing specific programmes)
G06F-0012/00 (Accessing, addressing or allocating within memory systems or architectures)

INSPEC Update Issue: 2004-047

Copyright: 2004, IEE

8/5/3 (Item 2 from file: 2)
DIALOG(R)File 2: INSPEC
(c) 2012 The IET. All rights reserved.

08935735

Title: **Square hash with a small key size**

Author(s): Swee-Huay Heng[1]; Kurosawa, K.

Affiliation(s):
[1] Tokyo Inst. of Technol., Japan

Journal: IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences , vol.E87-A , no.1 , pp.54-9

Publisher: Inst. Electron. Inf. & Commun. Eng.

Country of Publication: Japan

Publication Date: Jan. 2004

ISSN: 0916-8508

ISSN Type: print

SICI: 0916-8508(200401)E87A:1L.54:SHWS;1-7

CODEN: IFESEX

Language: English

Document Type: Journal Paper (JP)

Treatment: Theoretical or Mathematical (T)

Abstract: This paper shows an improvement of square hash function family proposed by Etzel et al. (1999). In the new variants, the size of keys is much shorter while the

collision probability is slightly larger. Most of the main techniques used to optimize the original square hash functions work on our variants as well. The proposed algorithms are applicable to fast and secure message authentication. (*15 refs.*)
Subfile(s): B (Electrical & Electronic Engineering); C (Computing & Control Engineering)
Descriptors: message authentication; public key cryptography
Identifiers: square hash; small key **size**; collision probability; secure **message** authentication; **message** authentication codes; universal **hash**
Classification Codes: B6120D (Cryptography); C6130S (Data security); C1260C (Cryptography theory)
International Patent Classification:
G06F-0021/00 (Security arrangements for protecting computers or computer systems against unauthorised activity)
H04L-0009/00 (Arrangements for secret or secure communication)
INSPEC Update Issue: 2004-016

Copyright: 2004, IEE

8/5/4 (Item 3 from file: 2)
DIALOG(R)File 2: INSPEC

08892684
Title: An IP address based caching scheme for peer-to-peer networks
Author(s): Ferreira, R.A.[1]; Grama, A.[1]; Jagannathan, S.[1]
Affiliation(s):
[1] Dept. of Comput. Sci., Purdue Univ., West Lafayette, IN, USA
Book Title: GLOBECOM '03. IEEE Global Telecommunications Conference (IEEE Cat. No.03CH37489)
Inclusive Page Numbers: 3845-50 vol.7
Publisher: IEEE, Piscataway, NJ
Country of Publication: USA
Publication Date: 2003
Conference Title: GLOBECOM '03. IEEE Global Telecommunications Conference
Conference Date: 1-5 Dec. 2003
Conference Location: San Francisco, CA, USA
ISBN: 0-7803-7974-8
U.S. Copyright Clearance Center Code: 0-7803-7974-8/03/$17.00
Part: vol.7
Number of Pages: cv+4209
Language: English
Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: Distributed hash tables (DHTs), used in a number of current peer-to-peer systems, provide efficient mechanisms for resource location. Systems such as Chord,

Pastry, CAN, and Tapestry provide strong guarantees that queries in the overlay network can be resolved in a bounded number of overlay hops, while preserving load balance among the peers. A key distinction in these systems is the way they handle locality in the underlying network. Topology-based node identifier assignment, proximity routing, and proximity neighbor selection are examples of heuristics used to minimize message delays in the underlying network. We investigate the use of source IP addresses to enhance locality in overlay networks based on DHTs. We first show that a naive use of source IP address potentially leads to severe resource imbalance due to nonuniformity of peers over the IP space. We then present an effective caching scheme that combines a segment of the source IP with the queried hash-code to localize access and affect replication effectively. Using detailed experiments, we show that this scheme achieves performance gains of up to 41%, when compared to Pastry in combination with the proximity neighbor selection heuristic. (*24 refs.*)
Subfile(s): B (Electrical & Electronic Engineering); C (Computing & Control Engineering)
Descriptors: delays; Internet; IP networks; minimisation; network topology; telecommunication network routing
Identifiers: source IP address; caching scheme; peer-to-peer networks; distributed hash tables; DHT; resource location; Chord; Pastry; Tapestry; CAN; content-addressable network; overlay network; node identifier assignment; proximity routing; proximity neighbor selection; heuristics; **message** delay minimization; IP **space**; **hash**-code; Internet
Classification Codes: B6210L (Computer communications); B6150P (Communication network design, planning and routing); C5620W (Other computer networks)
International Patent Classification:
H04L-0012/28 (Characterised by path configuration, e.g. lan [local area networks] or wan [wide area networks])
H04W-0016/00 (Network planning, e.g. coverage or traffic planning tools; Network deployment, e.g. resource partitioning or cell structures)
H04W-0040/00 (Communication routing or communication path finding)
INSPEC Update Issue: 2004-010

Copyright: 2004, IEE

8/5/5 (Item 4 from file: 2)
DIALOG(R)File 2: INSPEC

08839550
Title: Assuring consistency and increasing reliability in group communication mechanisms in computational resiliency
Author(s): Lucena, N.[1]; Chapin, S.J.[1]; Lee, J.
Affiliation(s):
[1] Syst. Assurance Inst., Syracuse Univ., NY, USA
Book Title: IEEE Systems, Man and Cybernetics Society Information Assurance

Workshop (IEEE Cat. No.03EX676)
Inclusive Page Numbers: 135-42
Publisher: IEEE, Piscataway, NJ
Country of Publication: USA
Publication Date: 2003
Conference Title: IEEE Systems, Man and Cybernetics Society Information Assurance Workshop
Conference Date: 18-20 June 2003
Conference Location: West Point, NY, USA
ISBN: 0-7803-7808-3
U.S. Copyright Clearance Center Code: 0-7803-7808-3/03/$17.00
Number of Pages: 307
Language: English
Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: The computational resiliency library (CRLib) provides distributed systems with the ability to sustain operation and dynamically restore the level of assurance in system function during attacks or failures. In the presence of arbitrary faults, replicated threads need to agree on the values received in order to achieve consistency, when doing group communication in CRLib. To guarantee data integrity and increase reliability, we have implemented a variant of the Lamport-Shostak-Pease oral message algorithm for the Byzantine Generals problem, which provides fuzzy agreement as well as a reduction of the expected communication overhead. Instead of agreeing on the original messages, which could be extremely large, agreement is performed over the 160-bit **hashes** of normalized **messages** computed using SHA-1. Performance **measurements** of applications using CRLib supporting both fail-stop and arbitrary failure models indicate that a reasonable overhead in execution time is worth paying in cases when Byzantine failures are expected. (*18 refs.*)
Subfile(s): C (Computing & Control Engineering)
Descriptors: communication complexity; computer crime; data integrity; groupware; message passing; multi-threading; software libraries
Identifiers: computational resiliency library; distributed information system; assurance consistency; system function; replicated thread; group communication mechanism reliability; data integrity; Lamport-Shostak-Pease algorithm; Byzantine problem; fuzzy agreement; communication overhead; performance measurement; SHA-1
Classification Codes: C6150N (Distributed systems software); C6130S (Data security); C6110B (Software engineering techniques); C4240C (Computational complexity); C6130G (Groupware)
International Patent Classification:
G06F-0009/44 (Arrangements for executing specific programmes)
G06F-0021/00 (Security arrangements for protecting computers or computer systems against unauthorised activity)
INSPEC Update Issue: 2004-003

8/5/6 (Item 5 from file: 2)
DIALOG(R)File 2: INSPEC

08686596
Title: **Secure communication based on elliptic curve public key cryptosystems (II)**
Author(s): Petac, E.
Journal: Buletinul Institutului Politehnic din Iasi, Sectia III (Electrotehnica, Energetica, Electronica) , vol.46 , no.1-2 , pp.87-95
Publisher: Inst. Politeh. Iasi
Country of Publication: Romania
Publication Date: 2000
ISSN: 0258-9109
ISSN Type: print
SICI: 0258-9109(2000)46:1/2L.87:SCBE;1-K
CODEN: BIEAEP
Language: English
Document Type: Journal Paper (JP)
Treatment: Theoretical or Mathematical (T)
Abstract: The cryptographic importance of the elliptic curve public key cryptosystems (ECPKC) consists of the difficulty in determining discrete logarithms over extensions of finite fields. This is much harder than factorization of integers or calculating discrete logarithms in F_q. Another most important aspect consists in the forms for the private keys and for the public keys; the private keys are ordinary integers and the public keys are points on an elliptic curve. Elliptic curve systems are very good for applications with smart cards and in distributed systems, where computational power and integrated circuit space are limited, because computations are easily performed and bandwidth requirements are minimal. The paper presents an elliptic curve authenticated encryption scheme using a universal hash function (UHF). The UHF can take an input octet string message M of arbitrary length. The output of the UHF is an octet string H of 64 bits fixed length. For computing in finite extensions over finite rings we have used the ZEN-new toolbox, where there are some computing routines implementing the group law defined for an elliptic curve. (*13 refs.*)
Subfile(s): B (Electrical & Electronic Engineering); C (Computing & Control Engineering)
Descriptors: elliptic equations; message authentication; public key cryptography; smart cards
Identifiers: PKC; authentication; secure communication; elliptic curve public key cryptosystems; ECPKC; discrete logarithm determination; finite field extensions; integer private keys; elliptic curve points; public keys; smart cards; distributed systems; computational power; IC **space** limitations; authenticated encryption schemes; universal **hash** functions; input octet string **messages**; arbitrary length string messages; fixed octet string length; finite rings; elliptic curve group laws; 64 bit
Classification Codes: B6120D (Cryptography); B0290P (Differential equations (numerical analysis)); C1260C (Cryptography theory); C6130S (Data security); C4170 (

Differential equations (numerical analysis))
International Patent Classification:
G06F-0021/00 (Security arrangements for protecting computers or computer systems against unauthorised activity)
G06K-0019/07 (With integrated circuit chips)
H04L-0009/00 (Arrangements for secret or secure communication)
Numerical Indexing: word length: 6.4E+01 bit
INSPEC Update Issue: 2003-028

8/5/7 (Item 6 from file: 2)
DIALOG(R)File 2: INSPEC

08658358
Title: An efficient MAC for short messages
Author(s): Patel, S.[1]
Affiliation(s):
[1] Lucent Technol. Bell Labs., Whippany, NJ, USA
Book Title: Selected Areas in Cryptography. 9th Annual International Workshop, SAC 2002. Revised Papers (Lecture Notes in Computer Science Vol.2595)
Inclusive Page Numbers: 353-68
Publisher: Springer-Verlag, Berlin
Country of Publication: Germany
Publication Date: 2003
Conference Title: SAC 2002. Selected Areas in Cryptography
Conference Date: 15-16 Aug. 2002
Conference Location: St. John's, Nfld., Canada
Editor(s): Nyberg, K. Heys, H.
ISBN: 3-540-00622-2
Number of Pages: xi+404
Language: English
Document Type: Conference Paper (PA)
Treatment: Theoretical or Mathematical (T)
Abstract: HMAC is the Internet standard for message authentication. What distinguishes HMAC from other MAC algorithms is that it provides proofs of security assuming that the underlying cryptographic hash (e.g. SHA-1) has some reasonable properties. HMAC is efficient for long messages, however, for short messages the nested constructions results in a significant inefficiency. For example to MAC a message shorter than a block, HMAC requires at least two calls to the compression function rather than one. This inefficiency may be particularly high for some applications, like message authentication of signaling messages, where the individual messages may all fit within one or two blocks. Also for TCP/IP traffic it is well known that a large number of packets (e.g. acknowledgement) have sizes around 40 bytes

which fit within a block of most cryptographic hashes. We propose an enhancement that allows both short and long messages to be message authenticated more efficiently than HMAC while also providing proofs of security. In particular, for a message smaller than a block our MAC only requires one call to the compression function. (*9 refs.*)
Subfile(s): B (Electrical & Electronic Engineering); C (Computing & Control Engineering)
Descriptors: cryptography; Internet; message authentication; telecommunication security; telecommunication traffic; transport protocols
Identifiers: MAC; short messages; HMAC; internet standard; **message** authentication; MAC algorithms; security; cryptographic **hash**; compression function; signaling **messages**; TCP/IP traffic; packet **size**; acknowledgement; message authentication code; SHA-1
Classification Codes: B6120D (Cryptography); B6150M (Protocols); B6210L (Computer communications); C1260C (Cryptography theory); C6130S (Data security); C5640 (Protocols); C5620W (Other computer networks)
International Patent Classification:
G06F-0021/00 (Security arrangements for protecting computers or computer systems against unauthorised activity)
H04K-0001/00 (Secret communication)
H04L-0009/00 (Arrangements for secret or secure communication)
H04L-0012/28 (Characterised by path configuration, e.g. lan [local area networks] or wan [wide area networks])
H04W-0012/00 (Security arrangements, e.g. access security or fraud detection; Authentication, e.g. verifying user identity or authorisation; Protecting privacy or anonymity)
INSPEC Update Issue: 2003-023

8/5/8 (Item 7 from file: 2)
DIALOG(R)File 2: INSPEC

08387256
Title: Performance analysis of IPSec protocol: encryption and authentication
Author(s): Elkeelany, O.[1]; Matalgah, M.M.; Sheikh, K.P.; Thaker, M.; Chaudhry, G.; Medhi, D.; Qaddour, J.
Affiliation(s):
[1] Missouri Univ., Kansas City, MO, USA
Book Title: 2002 IEEE International Conference on Communications. Conference Proceedings. ICC 2002 (Cat. No.02CH37333)
Inclusive Page Numbers: 1164-8 vol.2
Publisher: IEEE, Piscataway, NJ
Country of Publication: USA
Publication Date: 2002

Conference Title: Proceedings of IEEE International Conference on Communications
Conference Date: 28 April-2 May 2002
Conference Location: New York, NY, USA
ISBN: 0-7803-7400-2
U.S. Copyright Clearance Center Code: 0-7803-7400-2/02/$17.00
Medium: Also available on CD-ROM in PDF format
Item Identifier (DOI): 10.1109/ICC.2002.997033
Part: vol.2
Number of Pages: 5 vol.lvi+3456
Language: English
Document Type: Conference Paper (PA)
Treatment: Theoretical or Mathematical (T)
Abstract: IPSec provides two types of security algorithms, symmetric encryption algorithms (e.g. data encryption standard DES) for encryption, and one-way hash functions (e.g., message digest MD5 and secured hash algorithm SHA1) for authentication. This paper presents performance analysis and comparisons between these algorithms in terms of time complexity and space complexity. Parameters considered are processing power and input size. The analysis results revealed that HMAC-MD5 can be sufficient for the authentication purposes rather than using the more complicated HMAC-SHA1 algorithm. In encryption applications, authentication should be combined with DES. (*13 refs.*)
Subfile(s): B (Electrical & Electronic Engineering); C (Computing & Control Engineering)
Descriptors: computational complexity; cryptography; message authentication; telecommunication security; transport protocols
Identifiers: performance analysis; IPSec protocol; encryption; authentication; security algorithms; symmetric encryption algorithms; data encryption standard; DES; one-way **hash** functions; **message** digest; secured **hash** algorithm; time complexity; **space** complexity; processing power; input size; HMAC-MD5; HMAC-SHA1 algorithm
Classification Codes: B6150M (Protocols); B6120D (Cryptography); C5640 (Protocols); C6130S (Data security)
International Patent Classification:
G06F-0021/00 (Security arrangements for protecting computers or computer systems against unauthorised activity)
H04K-0001/00 (Secret communication)
H04L-0009/00 (Arrangements for secret or secure communication)
H04W-0012/00 (Security arrangements, e.g. access security or fraud detection; Authentication, e.g. verifying user identity or authorisation; Protecting privacy or anonymity)
INSPEC Update Issue: 2002-037

8/5/9 (Item 8 from file: 2)
DIALOG(R)File 2: INSPEC

08342634
Title: **Optimal security proofs for PSS and other signature schemes**
Author(s): Coron, J.-S.[1]
Affiliation(s):
[1] Gemplus Card Int., Issy-les-Moulineaux, France
Book Title: Advances in Cryptology - EUROCRYPT 2002. International Conference on the Theory and Applications of Cryptographic Techniques. Proceedings (Lecture Notes in Computer Science Vol.2332)
Inclusive Page Numbers: 272-87
Publisher: Springr-Verlag, Berlin
Country of Publication: Germany
Publication Date: 2002
Conference Title: Advances in Cryptology - EUROCRYPT 2002. International Conference on the Theory and Applications of Cryptographic Techniques. Proceedings
Conference Date: 28 April-2 May 2002
Conference Location: Amsterdam, Netherlands
Editor(s): Knudsen, L.
ISBN: 3-540-43553-0
Number of Pages: xii+545
Language: English
Document Type: Conference Paper (PA)
Treatment: Theoretical or Mathematical (T)
Abstract: The probabilistic signature scheme (PSS) designed by Bellare and Rogaway (1993, 1996) is a signature scheme provably secure against chosen message attacks in the random oracle model, whose security can be tightly related to the security of RSA. We derive a new security proof for PSS in which a much shorter random salt is used to achieve the same security level, namely we show that $\log_2 q_{sig}$ bits suffice, where q_{sig} is the number of signature queries made by the attacker. When PSS is used with message recovery, a better bandwidth is obtained because longer messages can now be recovered. We also introduce a new technique for proving that the security proof of a signature scheme is optimal. In particular, we show that the size of the random salt that we have obtained for PSS is optimal: if less than $\log_2 q_{sig}$ bits are used, then PSS is still provably secure but it cannot have a tight security proof. Our technique applies to other signature schemes such as the full domain hash scheme and Gennaro-Halevi-Rabin's (see Eurocrypt '99, LNCS vol.1592, p.123-39, 1999) scheme, whose security proofs are shown to be optimal. (*20 refs.*)
Subfile(s): B (Electrical & Electronic Engineering); C (Computing & Control Engineering)
Descriptors: optimisation; probability; public key cryptography; random processes
Identifiers: optimal security proofs; signature schemes; PSS; probabilistic signature scheme; message attacks; random oracle model; random salt **size**; signature queries; **message** recovery; bandwidth; full domain **hash** scheme; Gennaro-Halevi-Rabin's scheme; public-key cryptography; RSA
Classification Codes: B6120D (Cryptography); B0260 (Optimisation techniques);

B0240Z (Other topics in statistics); C1260C (Cryptography theory); C6130S (Data security) ; C1180 (Optimisation techniques); C1140Z (Other topics in statistics)
International Patent Classification:
G06F-0021/00 (Security arrangements for protecting computers or computer systems against unauthorised activity)
H04L-0009/00 (Arrangements for secret or secure communication)
INSPEC Update Issue: 2002-030

Copyright: 2002, IEE

8/5/10 (Item 9 from file: 2)
DIALOG(R)File 2: INSPEC

06704603
Title: Dynamic word based text compression
Author(s): Ng, K.S.[1]; Cheng, L.M.[1]; Wong, C.H.[1]
Affiliation(s):
[1] Dept. of Electron. Eng., City Univ. of Hong Kong, Kowloon, Hong Kong
Book Title: Proceedings of the Fourth International Conference on Document Analysis and Recognition (Cat. No.97TB100138)
Inclusive Page Numbers: 412-16 vol.1
Publisher: IEEE Comput. Soc., Los Alamitos, CA
Country of Publication: USA
Publication Date: 1997
Conference Title: Proceedings of the Fourth International Conference on Document Analysis and Recognition
Conference Date: 18-20 Aug. 1997
Conference Location: Ulm, Germany
Conference Sponsor: Int. Assoc. Pattern Recognition (IAPR), TC 10 & 11 Int. Graphonomics Soc. (IGS) German Assoc. Comput. Sci. (GI) German Assoc. Inf. Technol. (ITG)
ISBN: 0-8186-7898-4
U.S. Copyright Clearance Center Code: 0 8186 7898 4/97/$10.00
Item Identifier (DOI): 10.1109/ICDAR.1997.619880
Part: vol.1
Number of Pages: 2 vol. xxiv+1119
Language: English
Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: We propose a dynamic text compression technique with a back searching algorithm and a new storage protocol. Codes being encoded are divided into three types namely copy, literal and hybrid codes. Multiple dictionaries are adopted and each of them has a linked sub-dictionary. Each dictionary has a portion of pre-defined words i.e. the most frequent words and the rest of the entries will depend on the message. A

hashing function developed by Pearson (1990) is adopted. It serves two purposes. Firstly, it is used to initialize the dictionary. Secondly, it is used as a quick search to a particular word. By using this scheme, the spaces between words do not need to be considered. At the decoding side, a space character will be appended after each word is decoded. Therefore, the redundancy of space can also be compressed. The result shows that the original message will not be expanded even if we have poor dictionary design. (*8 refs.*)
Subfile(s): C (Computing & Control Engineering)
Descriptors: backtracking; data compression; document image processing; file organisation; glossaries; image coding; memory protocols; search problems
Identifiers: dynamic word based text compression; back searching algorithm; storage protocol; dictionaries; encoding; copy codes; literal codes; hybrid codes; **hashing** function; decoding; **space** character; redundancy; **message**
Classification Codes: C6130D (Document processing techniques); C5260B (Computer vision and image processing techniques); C1250 (Pattern recognition); C6120 (File organisation)
International Patent Classification:
G06F-0012/00 (Accessing, addressing or allocating within memory systems or architectures)
G06F-0017/21 (Text processing)
G06T (Image data processing or generation, in general)
G06T-0009/00 (Image coding, e.g. from bit-mapped to non bit-mapped)
INSPEC Update Issue: 1997-038

Copyright: 1997, IEE

8/5/11 (Item 10 from file: 2)
DIALOG(R)File 2: INSPEC
(c) 2012 The IET. All rights reserved.

06659155
Title: **Fast message authentication using efficient polynomial evaluation**
Author(s): Afanassiev, V.[1]; Gehrmann, C.; Smeets, B.
Affiliation(s):
[1] Inst. of Problems of Inf. Transmission, Acad. of Sci., Moscow, Russia
Book Title: Fast Software Encryption. 4th International Workshop, FSE '97 Proceedings
Inclusive Page Numbers: 190-204
Publisher: Spriner-Verlag, Berlin
Country of Publication: Germany
Publication Date: 1997
Conference Title: Fast Software Encryption. 4th International Workshop, FSE'97 Proceedings
Conference Date: 20-22 Jan. 1997
Conference Location: Haifa, Israel

Editor(s): Biham, E.

ISBN: 3-540-63247-6

Number of Pages: viii+287

Language: English

Document Type: Conference Paper (PA)

Treatment: Practical (P)

Abstract: Message authentication codes (MACs) using polynomial evaluation have the advantage of requiring a very short key, even for very large messages. We describe a low-complexity software polynomial evaluation procedure that, for large message sizes, gives a MAC that has about the same low software complexity as for bucket hashing but requires only small keys and has better security characteristics. (*21 refs.*)

Subfile(s): B (Electrical & Electronic Engineering); C (Computing & Control Engineering)

Descriptors: computational complexity; cryptography; message authentication; polynomials

Identifiers: fast message authentication; polynomial evaluation procedure; message authentication codes; short key; software complexity; large **message sizes**; bucket **hashing**; security characteristics; universal hash functions; software MAC generation

Classification Codes: B6120B (Codes); B0210 (Algebra); C6130S (Data security); C4240C (Computational complexity); C1110 (Algebra)

International Patent Classification:
G06F-0021/00 (Security arrangements for protecting computers or computer systems against unauthorised activity)
H03M (Coding, decoding or code conversion, in general)

INSPEC Update Issue: 1997-031

8/5/12 (Item 11 from file: 2)
DIALOG(R)File 2: INSPEC

06659154

Title: **MMH: software message authentication in the Gbit/second rates**

Author(s): Halevi, S.[1]; Krawczyk, H.

Affiliation(s):
[1] Lab. for Comput. Sci., MIT, Cambridge, MA, USA

Book Title: Fast Software Encryption. 4th International Workshop, FSE '97 Proceedings

Inclusive Page Numbers: 172-89

Publisher: Spriner-Verlag, Berlin

Country of Publication: Germany

Publication Date: 1997

Conference Title: Fast Software Encryption. 4th International Workshop, FSE'97 Proceedings

Conference Date: 20-22 Jan. 1997
Conference Location: Haifa, Israel
Editor(s): Biham, E.
ISBN: 3-540-63247-6
Number of Pages: viii+287
Language: English
Document Type: Conference Paper (PA)
Treatment: Practical (P)

Abstract: Describes MMH (multilinear modular hashing), a construction of almost universal hash functions that is suitable for very fast software implementation and is applicable to the hashing of variable-size data and fast cryptographic message authentication. Our construction uses fast single-precision arithmetic (which is increasingly supported by modern processors due to the growing needs for fast arithmetic posed by multimedia applications). We report on hand-optimized assembly implementations on a 150-MHz PowerPC 604 and a 150-MHz Pentium-Pro, which achieve hashing speeds of 350 to 820 Mbit/s, depending on the desired level of security (or collision probability), and a rate of more than 1 Gbit/s on a 200 MHz Pentium-Pro. This represents a significant speed-up over current software implementations of universal hashing and other message authentication techniques (e.g. MD5-based). Moreover, our construction is specifically designed to take advantage of emerging microprocessor technologies (such as Intel's MMX, 64-bit architectures and others), and is best suited to accommodate the growing performance needs of cryptographic (and other universal hashing) applications. The construction is based on techniques due to Carter and Wegman (1979) for universal hashing using modular multilinear functions that we have carefully modified to allow for fast software implementation. We prove that the resultant construction retains the necessary mathematical properties required for its use in hashing and message authentication. (*19 refs.*)

Subfile(s): B (Electrical & Electronic Engineering); C (Computing & Control Engineering)
Descriptors: cryptography; digital arithmetic; message authentication; microcomputer applications; multimedia systems
Identifiers: MMH; multilinear modular **hashing**; software **message** authentication; almost universal **hash** functions; fast software implementation; variable-**size** data; cryptography; single-precision arithmetic; multimedia applications; hand-optimized assembly implementations; PowerPC 604; Pentium-Pro; hashing speed; security; collision probability; Intel MMX; 64-bit architectures; microprocessor technologies; performance needs; modular multilinear functions; mathematical properties; 150 MHz; 350 to 820 Mbit/s; 1 Gbit/s; 200 MHz; 64 bit
Classification Codes: B6120B (Codes); B6210R (Multimedia communications); C6130S (Data security); C6130M (Multimedia); C5230 (Digital arithmetic methods)
International Patent Classification:
H04N (Pictorial communication, e.g. television)
G06F-0021/00 (Security arrangements for protecting computers or computer systems against unauthorised activity)
H03M (Coding, decoding or code conversion, in general)
Numerical Indexing: bit rate: 3.5E+08 to 8.2E+08 bit/s; word length: 6.4E+01 bit;

frequency: 1.5E+08 Hz; frequency: 2.0E+08 Hz; bit rate: 1.0E+09 bit/s
INSPEC Update Issue: 1997-031

Copyright: 1997, IEE

8/5/13 (Item 12 from file: 2)
DIALOG(R)File 2: INSPEC
(c) 2012 The IET. All rights reserved.

06541031
Title: **LH*-a scalable, distributed data structure**
Author(s): Litwin, W.[1]; Neimat, M.-A.[1]; Schneider, D.A.[1]
Affiliation(s):
[1] Hewlett-Packard Co., Palo Alto, CA, USA
Journal: ACM Transactions on Database Systems , vol.21 , no.4 , pp.480-525
Publisher: ACM
Country of Publication: USA
Publication Date: Dec. 1996
ISSN: 0362-5915
ISSN Type: print
SICI: 0362-5915(199612)21:4L.480:SDDS;1-C
CODEN: ATDSD3
U.S. Copyright Clearance Center Code: 0362-5915/96/1200-0480$03.50
Language: English
Document Type: Journal Paper (JP)
Treatment: Practical (P); Theoretical or Mathematical (T)
Abstract: We present a scalable distributed data structure called LH*. LH* generalizes Linear Hashing (LH) to distributed RAM and disk files. An LH* file can be created from records with primary keys, or objects with OIDs, provided by any number of distributed and autonomous clients. It does not require a central directory, and grows gracefully, through splits of one bucket at a time, to virtually any number of servers. The number of messages per random insertion is one in general, and three in the worst case, regardless of the file size. The number of messages per key search is two in general, and four in the worst case. The file supports parallel operations, e.g., hash joins and scans. Performing a parallel operation on a file of M buckets costs at most 2M+1 messages, and between 1 and O($\log_2$M) rounds of messages. We first describe the basic LH* scheme where a coordinator site manages bucket splits, and splits a bucket every time a collision occurs. We show that the average load factor of an LH* file is 65-70% regardless of file size, and bucket capacity. We then enhance the scheme with load control, performed at no additional message cost. We next define LH* schemes without a coordinator. We show that insert and search costs are the same as for the basic scheme. Next, we briefly describe two variants of splitting policy, using parallel splits and presplitting that should enhance performance for high-performance applications. (*29 refs.*)
Subfile(s): C (Computing & Control Engineering)

Descriptors: client-server systems; data structures; database theory; distributed databases; software performance evaluation
Identifiers: LH*; scalable distributed data structure; Linear Hashing; distributed RAM; disk files; distributed clients; servers; **messages**; file **size**; parallel operations; **hash** joins; scans; parallel operation; coordinator site; bucket splits; average load factor; load control; search costs; splitting policy; performance; client server systems
Classification Codes: C6160B (Distributed databases); C4250 (Database theory); C6120 (File organisation)
International Patent Classification:
G06F-0012/00 (Accessing, addressing or allocating within memory systems or architectures)
G06F-0017/30 (Information retrieval; Database structures therefor)
INSPEC Update Issue: 1997-014

8/5/14 (Item 1 from file: 144)
DIALOG(R)File 144: Pascal

16118400 PASCAL No.: 03-0277027

Comparative analysis of the hardware implementations of hash functions SHA-1 and SHA-512 Information security : Sao Paulo, 30 September - 2 October 2002

GREMBOWSKI Tim; LIEN Roar; GAJ Kris; NGUYEN Nghi; BELLOWS Peter; FLIDR Jaroslav; LEHMAN Tom; SCHOTT Brian
CHAN Agnes Hui, ed; GLIGOR Virgil, ed
Electrical and Computer Engineering, George Mason University, 4400 University Drive, Fairfax, VA 22030, United States; University of Southern California-Information Sciences Institute, Arlington, VA 22203, United States

ISC 2002 : internation conference on information security, 5 (Sao Paulo BRA) 2002-09-30
Journal: Lecture notes in computer science,
2002, 2433 75-89
ISBN: 3-540-44270-7 ISSN: 0302-9743 Availability:
INIST-16343; 354000108470370060
No. of Refs.: 17 ref.
Document Type: P (Serial); C (Conference Proceedings) ; A (Analytic)
Country of Publication: Germany
Language: English

Hash functions are among the most widespread cryptographic primitives, and are currently used in multiple cryptographic schemes and security protocols such as IPSec and SSL. In this paper, we compare and contrast hardware implementations of the newly proposed draft hash standard SHA-512, and the old standard, SHA-1. In our implementation based on Xilinx Virtex FPGAs, the throughput of SHA-512 is equal to 670 Mbit/s, compared to 530

Mbit/s for SHA-1. Our analysis shows that the newly proposed hash standard is not only orders of magnitude more secure, but also significantly faster than the old standard. The basic iterative architectures of both hash functions are faster than the basic iterative architectures of symmetric-key ciphers with equivalent security.

English Descriptors: Security key; Iterative method; Cryptography;
Transmission protocol; Field programmable gate array; Channel **capacity**; Implementation; **Message** authentication; **Hash** function

French Descriptors: Cle securite; Methode iterative; Cryptographie;
Protocole transmission; Reseau porte programmable; Capacite canal; Implementation; Authentification message; Fonction hachage

Classification Codes: 001D04A04E

8/5/15 (Item 1 from file: 56)
DIALOG(R)File 56: Computer and Information Systems Abstracts

0000721059 IP Accession No: 200802-80-049049
Divide and concatenate:a scalable hardware architecture for universal MAC

Yang, Bo; Karri, Ramesh; McGrew, David A Polytechnic University, Brooklyn, NY
, p 258-258 , 2004
Publication Date: 2004
Publisher: Association for Computing Machinery, Inc. , One Astor Plaza, 1515 Broadway , New York , NY , 10036-5701
Country Of Publication: USA
Publisher Url:
http://portal.acm.org/citation.cfm?id=968280.968353&coll=ACM&dl=ACM &type=series&idx=SERIES100&part=series&WantType=Proceedings&title=FPGA&CFID=6135546 &CFTOKEN=84105396; http://www.acm.org/
Publisher Email: SIGS@acm.org

Conference:
International Symposium on Field Programmable Gate Arrays: Proceedings of the 2004 ACM/SIGDA 12th international symposium on Field programmable gate arrays , 22-24 Feb. 2004

Document Type: Conference Paper
Record Type: Abstract

Language: English
ISBN: 1581138296
Notes: Monterey, California, USA
DOI: 10.1145/968280.968353
File Segment: Computer & Information Systems Abstracts

Abstract:

We present a cryptographic architecture optimization technique called divide-and-concatenate based on two observations: (i) the area of a multiplier and associated data path decreases quadratically and their speeds increase gradually as their operand **size** is reduced. (ii) in **hash** functions, **message** authentication codes and related cryptographic algorithms, two functions are equivalent if they have the same collision probability property. In the proposed approach we divide a 2w-bit data path into two w-bit data paths and concatenate their results to construct an equivalent 2w-bit data path. We applied this technique on NH hash. When compared to the 100% overhead associated with duplicating a straightforward 32-bit pipelined NH hash data path, the divide-and-concatenate approach yields a 94% increase in throughput with only 40% hardware overhead. The NH hash associated message authentication code UMAC architecture with collision probability 2-32 that uses four equivalent 8-bit divide-and-concatenate NH hash data paths yields a throughput of 79.2 Gbps with only 3840 FPGA slices when implemented on a Xilinx FPGA.

Descriptors: Data paths; Hash based algorithms; Field programmable gate arrays; Equivalence; Architecture; Hardware; Messages; Cryptography; Authentication ; Reproduction; Polytechnics; Algorithms; Tungsten; Construction; Multipliers
Subj Catg: 80, Computer Applications (General)

8/5/16 (Item 1 from file: 60)
DIALOG(R)File 60: ANTE: Abstracts in New Tech & Engineer

0000487975 IP Accession No: 2008084222
Digital Certificate

Tycksen Jr, Frank A; Jennings, Charles W
, USA
Publisher Url: http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u =/netaht ml/PTO/search-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=61 89097.PN.&OS=pn/6189097&RS=PN/6189097

Document Type: Patent
Record Type: Abstract
Language: English
File Segment: ANTE: Abstracts in New Technologies and Engineering

Abstract:
A digital certificate includes framing characters defining a protected area. The protected area contains a selected set of components, including text-based components and binary-based components, and the certificate serves as a transport container for such components. A **message** digest or **hashing** algorithm applied to the protected **area** provides consistent results despite modifications to the certificate outside the protected area. A digital signature provides authentication of source and content integrity. Digital certificates under the present invention may be applied to a variety of purposes including but not limited to proof of ownership, gift certificates, upgrade purchases, and other applications where verification of source and content integrity are desirable.

Descriptors: Digital certificates; Messages; Framing; Inventions; Authentication; Transport; Algorithms; Digital signatures; Ownership; Containers; Proving

Inventors: **Tycksen, Jr.; Frank A.** (Beaverton, OR)**, Jennings; Charles W.** (Portland, OR) Assignee: **Preview Systems, Inc.** (Sunnyvale, CA)
Appl. No.: **08/822,661** Filed: **March 24, 1997**

7/5/3 (Item 1 from file: 636)
DIALOG(R)File 636: Gale Group Newsletter DB(TM)

02481513 **Supplier Number:** 44977961 **(THIS IS THE FULLTEXT)**

IMPLEMENTATION AGREEMENTS EMERGE FROM NORTH AMERICA

Communications Standards News , n 183 , p N/A
Sept 7 , 1994
ISSN: 1077-4696
Language: English **Record Type:** Fulltext
Document Type: Newsletter ; Trade
Word Count: 765

Text:
The work of the Open Systems Environment Implementors Workshop (OIW) has resulted in an updated set of stable implementors agreements for open systems security in the US.
Part 12 of the "Stable Implementation Agreements for Open Systems Security" provides a framework for the development of protocol-specific security profiles. It covers distributed information processing in OSI application environments which are heterogeneous in terms of technology and administration.

The relationship between protocols and security is accomplished by developing a security profile that binds these areas together. Security profiles define protocol-specific implementations of security architectures by specifying a grouping of the security services to be offered, the placement of those services and the selection of the mechanisms to support them.

...Security Classes

The OIW Agreements define a set of security classes to provide a framework on which to build security profiles. Each class specifies the required security services in a generic form and for each application profile, one or more specific security services are chosen for each class.

The classes are organized into two similar hierarchies as shown in the table below. Each level of each hierarchy is a superset of the security services required of the immediately preceding level.

For each level in the hierarchies the same set of security services are required, except that one hierarchy includes confidentiality services.

Each level of the confidentiality hierarchy is a superset of the other hierarchy at the same level. So for example, S0 = authentication + access control and S0A= S0 + confidentiality.

Also included is a list (or register) of security algorithms which implementors can choose from for product development for open systems security. This list includes the following types of algorithm:

* Message digests/Hash Algorithms (e.g. MD4, MD5, SHA)

These algorithms compute a fixed **size** digest (or **hashed** total) of a **message**.

* Reversible public-key algorithms (e.g. RSA)

These algorithms are known as asymmetric key algorithms: - separate keys are used for encryption and decryption. These algorithms can be used to provide both confidentiality and authentication/integrity (e.g. digital signatures). They are also an ideal class of algorithm for the secure distribution of cryptographic keys especially for highly distributed systems.

* Irreversible public-key algorithms (e.g. Digital Signature Algorithm - DSA or El Gamal)

This class of algorithms are not reversible hence different algorithms are used for confidentiality and authenticity. Some of them have been designed to provide signature functionality only. They also use two keys like the reversible public-key algorithms.

* Key Exchange (e.g. Diffie-Hellman)

The list contains a number of commonly-used key exchange mechanisms. These are used to agree upon and exchange some shared (secret) information which may be used to compute some common value that can typically be used as a cryptographic key.

* Signature algorithm combinations (e.g. RSA with MD4, DSA with SHA)

The list has a number of appropriate digital signature/hash algorithm combinations that are used in practice.

* Symmetric-key algorithms (e.g. DES, RC2, RC4)

The list contains a number of symmetric-key encryption algorithms. Unlike the reversible public-key algorithms, they only use a single key.

Consequently, they provide a confidentiality capability but not a digital signature capability.

...OSI Upper Layers Security

The latest version of the stable agreements addresses the provision of security services in the upper layers of the OSI model through the use of a number of currently existing mechanism standards. These include the use of a number of Peer Entity Authentication Mechanisms:

-- ACSE (Association Control Service Element) authentication to support two-way authentication.

-- The Directory System Authentication Framework (X.509) for simple and strong authentication

-- Other external mechanisms to support authentication services such as Kerberos V5.0

There are also Data Origin Authentication/Integrity Transformations like GULS (Generic Upper Layer Security) for encryption, sealing and signing data.

...Network management services

The approach to providing security services OSI Network Management takes into consideration the need for different levels of security services within different network management domains, and the near-term requirement for interoperability of network management entities over heterogeneous network types.

The prime threats to OSI Network Management in this respect are:

* the masquerading of a manager or agent entity * the fabrication or modification of Common Management

...Information Protocol (CMIP) data units

Other threats of secondary concern include: the disclosure of CMIP data units; and the replay, reordering, insertion or deletion of CMIP data units.

The agreements go on to define a set of basic services and a set of enhanced services to counter these threats.

Basic services include peer entity authentication, data origin authentication and connectionless integrity. Enhanced services embrace connectionless confidentiality and connection-oriented integrity with or without recovery.

Publisher Name: Phillips Business Information, Inc.
Industry Names: BUSN (Any type of business); TELC (Telecommunications)

7/5/4 (Item 1 from file: 148)
DIALOG(R)File 148: Gale Group Trade & Industry DB

11763289   **Supplier Number:** 57445133 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Public key infrastructure: end-to-end security.(includes related articles on application-layer security and smart cards)(public key cryptography)

King, Christopher M.
Business Communications Review , 27 , 11 , 50(5)
Nov , 1997
ISSN: 0162-3885
Language: English
Record Type: Fulltext; Abstract
Word Count: 3776   **Line Count:** 00321

Abstract: Public key cryptography, a technology that has been used by certain sectors of the US government for over a decade, can be used by network managers for both business and security applications. Public Key Infrastructures (PKIs) are already available from the suppliers of Internet browsers and servers. These can be used to address such business concerns as secure Web-based applications while corporate passwords are expected to be replaced by digital certificates.
Industry Codes/Names: BUSN Any type of business; TELC Telecommunications
Descriptors: Internet--Safety and security measures; Public key encryption--Usage; World Wide Web--Safety and security measures; Web sites--Safety and security measures
Product/Industry Names: 4811520 (Online Services)
Product/Industry Names: 4822 Telegraph & other communications
NAICS Codes: 514191 On-Line Information Services
File Segment: TI File 148

7/5/7 (Item 2 from file: 15)
DIALOG(R)File 15: ABI/Inform(R)

00621994   92-37096
****USE FORMAT 7 OR 9 FOR FULL TEXT****
Who Holds the Keys? Debating Data Encryption Standards

Lyons, John W.; Anderson, John C.; Hellman, Martin E.; Rivest, Ronald L.
Communications of the ACM   v35n7 pp: 32-54
Jul 1992
ISSN: 0001-0782 **Journal Code:** ACM
Document Type: Journal article **Language:** English **Length:** 22 Pages
Special Feature: Appendix Equations References
Word Count: 14387

Abstract:

The National Institute of Standards and Technology (NIST) introduced a newly developed Digital Signature Algorithm (DAS) as the public encryption standard. The Digital Signature standard proposed specifies a Digital Signature Algorithm appropriate for applications requiring a digital rather than written signature. The DSA digital signature is a pair of large numbers represented in a computer as strings of binary digits. The digital signature is a computer using a set of rules and a set of parameters enabling it to be used to verify the identity of the originator amd integrity of the data. NIST's proposal is only for a public key signature system. There are no specifications for privacy or the exchange of secret keys. NIST is working to resolve the negative comments about the standard and is investigating a national infrastructure that will support digital signature applications in a cost-effective manner.

Company Names:
National Institute of Standards & Technology
Geographic Names: US

Descriptors: Algorithms; Data encryption; Federal regulation; Standardization; Criticism
Classification Codes: 5140 (CN=Security); 9190 (CN=United States); 4310 (CN=Regulation)